COMPUTER BASED ENVIRONMENT CONTROLS

Macoveiciuc Pastorel [1]

Abstract

The aim of these notes is to give an overview of the main activities of computer based activities controls. The basic principles of computer controls should be common to all sectors and to most types of hardware and software. The absence of a common definition of computer control may, in part, be due to the relative newness of computer controls. A key feature of many organisations today is change. Although not necessarily the driver of change, IT is invariably an intrinsec component and much of the change would not be possible without IT. IT has had a major impact on social, economic and political factors throughout the world. Not only has it led to the creation of new professions but it has also revolutionised others, such as office work, or, when combined with robotics, manufacturing industries.

Keywords: control, risk assessment, computer environment, data testing, impact of computers on controls.

Most of the companies have computer-based accounting systems. The main area of analysis in this written report is to ensure a full and complete understanding of the controls in a computer-based environment, whether there is an impact on the assessment of risks, and the subsequent control procedures. This is very useful in auditing the computer based environment. The procedures regarding the risk assessment will involve the use of computer-assisted audit techniques (CAATs).

Within a computer environment there are two main categories of controls:

- General controls;
- Application controls.

The general controls include all policies and procedures that relate to applications and support the effective functioning of application controls. These apply to mainframe, mini-frame and end-user environments.

The general controls purposes are to:

- maintain the information integrity and data security;
- control over the following:
    - software acquisition, changing and maintenance;
    - network operations;
    - access security;
    - applications acquisition, development, and maintenance.

Types of general controls:

[1] PhD. Student, Academy of Economic Studies-Bucharest, e-mail: pastorel-iulian@yahoo.com

- Controls over application development: over the system design and program writing, good documentation, testing procedures (e.g. use of test data to identify program code errors, pilot running and parallel running of old and new systems), as well as segregation of duties so that operators are not involved in program development;
- Controls over program changes: are performed in order to ensure no unauthorized amendments and that changes are adequately tested, e.g. password protection of programs, comparison of production programs to controlled copies and approval of changes by users;
- Controls over installation and maintenance of system software: – many of the controls mentioned above are relevant, e.g. authorization of changes, good documentation, access controls and segregation of duties.

The computer environment is tidily linked to the 'end-user environment' and refers to the situation in which the users of the computer systems are involved in all stages of the system development. In this respect we can mention that the end-user environment is related to:

- *Administrative controls:* these are controls over 'data centre and network operations' and 'access security'. These include controls that:
    - prevent or detect errors during program execution, e.g. procedure manuals, libraries of programs, job scheduling, training and supervision; all these prevent errors such as using wrong data files or wrong versions of production programs;
    - prevent unauthorized amendments to data files, e.g. authorization of jobs prior to processing, back up and physical protection of files and access controls such as passwords ensure the continuity of operations, e.g. testing of back-up procedures, protection against fire and floods, virus checks, use of read only memory, maintenance of programs loggs.
- *System development controls:* these type of controls cover the areas of system software acquisition development and maintenance, program changing and application system acquisition, development and maintenance. The 'system software' refers to the operating system, database management systems and other software that increases the efficiency of processing. Application software refers to particular applications such as sales or wages. The controls over the development and maintenance of both types of software are similar and include:

Application controls

The procedures used within the application controls are manual or automated. These operate at a business process level and apply to the processing of transactions by individual applications.

The application controls main characteristics are:

- preventive or detective in nature;
- designed to ensure the integrity of the accounting records;

- relating to procedures used to initiate, record, process and report transactions or other financial data;
- helping ensure that transactions occurred are authorized, complete and accurately recorded and processed.

The application controls apply generally to data processing tasks such as sales, purchases and wages procedures. These are divided into the following categories:

- *Input controls:* document counts, batch control totals, manual scrutiny of documents to ensure they have been authorized. A common example of programmed controls over the accuracy and completeness of input are edit checks (data validation) when the software checks the data fields included on transactions. This is done by performing:
  - reasonability check, e.g. alphabetical characters in a sales invoice number field;
  - range check, e.g. no employee's weekly wage is more than € 1,000;
  - check digit, e.g. an extra character added to the account reference field on a purchase invoice to detect mistakes such as transposition errors during input;
  - when data is input via a keyboard, the software will often display a screen message if any of the above checks reveal an anomaly, e.g. 'Supplier account number does not exist'.
- *Processing controls:* e.g. a run-to-run control i.e. the totals from one processing run, plus the input totals from the second processing, should equal the result from the second processing run. Example: the beginning balances on the payables ledger plus the purchases invoices (processing run 1) less the cheques issued (processing run 2) should equal the closing balances on the purchases ledger.
- *Output controls:* batch processing matches input to output, therefore this is also a control over processing and output. Other examples of output controls include the controlled resubmission of rejected transactions or the review of exception reports (e.g. the wages exception report showing employees being paid more than € 500).
- *Master files and standing data controls:* for example a one-for-one checking of changes to master files, e.g. customer price changes are checked to an authorized list. A regular printout of master files such as the wages master file could be forwarded monthly to the personnel department to ensure employees listed have personnel records.

Risk assessment procedures using computer techniques

The computer-assisted risk assessments techniques are related to controls that are characterized by the application of control and audit procedures using the computer as an audit tool. These are known as CAATs and are normally placed in three main categories:

1. *Audit software:* computer programs used by the auditor to interrogate a client's computer files mainly for substantive testing. These can be further categorized into:

a. *Package programs (generalized audit software)*: these are pre-prepared programs for which the auditor will specify detailed requirements. These are written to be used on different types of computer systems, therefore the auditor will be able to perform data processing function which include reading computer files, selecting information and performing calculations.
b. *Purpose-written programs*: these perform specific functions based on auditor's choices. The auditor may have no option but to have this software developed, since package programs cannot be adapted to the client's system (however, this can be costly).
c. *Enquiry programs*: these are programs that are part of the client's system, often used to sort and print data and can be adapted for audit purposes, e.g. accounting software which may have search facilities on some modules, or that could be used for audit purposes such as searching for all customers with credit balances (on the customers' module) or all inventory items exceeding a specified value (on the inventory module).

Using this audit software, you can scrutinize large volumes of data and present results that can then be investigated further. The software consists of program logic needed to perform most of the functions required in case of an audit, such as:

- sample selection;
- reporting exceptional items;
- files comparison;
- analyzing, summarizing and stratifying data.

For example, this software can be used to determine which of the following functions you wish to use, and select the criteria. Example: review and audit the property plant & equipments process:

- Select a random sample of additions from the fixed asset master file. This allows you to trace the sample back to contracts and invoices to confirm existence.
- Report all additions more that are more expensive than €1,000.
- Compare fixed assets register from the beginning of the month with the one the end of the month in order to trace the disposals during the month.
- Trace the disposals identified back to evidence, such as sales invoice and disposal minute.
- Assess the reasonability of the depreciation expenses.

2. *Data testing*: consists of techniques used in conducting control procedures by entering data as a sample of transactions, into an entity's computer system and compare the results obtained with pre-defined results. The prime objective is to test the operation of application controls. In this respect it is ideal to arrange for the dummy data to be processed, fact that might include many error conditions. This is done in order to ensure that the client's application controls can identify particular problems. Examples of errors that might occur:
    - supplier account codes that do not exist;
    - sales invoices that contain addition errors;

- employees earning in excess of a certain limit;
- submitting data with incorrect batch control totals. The data without errors will also be included to ensure that the 'correct' transactions are properly processed.

The data test can be used 'live', during the client's normal production run, but the main disadvantage with this choice is represented by the danger of corrupting the client's master files. In order to avoid this, it is useful to use an integrated facility test. The alternative is to perform a special run outside normal processing, using copies of the client's master files. In this case, the danger of corrupting the client's files is avoided, however the level of assurance is lower that if the normal production programs have been used.

3. *Other techniques* There is an increasing number of other techniques that can be used. The main ones are:
    - *Integrated test facility*: the technique runs data test live; it involves the establishment of dummy records, such as departments or customer accounts to which the dummy data can be processed. These can then be ignored when the client records are printed out, and reversed out afterwards.
    - *Embedded audit facilities (embedded audit monitor)*: requires the auditor's own program code to be embedded into the client's application software. The embedded code is designed to perform audit functions and can be switched on at selected times or activated each time the application program is used. Embedded facilities can be used to:
        - Gather and store information relating to transactions at the time of processing for subsequent audit review. The selected transactions are written to audit files for subsequent examination, often called system control and review file.
        - Spot and record (for subsequent review) any items that are unusual. The transactions are marked by the a code when selection conditions are satisfied. This technique is also referred to as tagging. The attraction of embedded control and review facilities is obvious, as it equates to having a perpetual review of transactions. However, the set-up is costly and may require the to have an input at the system development stage.

Impact of computer-based systems on the general approach

The fact that systems are computer-based does not alter the key stages of the review process. This explains why references to the computer-based systems have been subsumed into the following:

(i) *Planning*: represents one of the characteristics of the review and control process that needs to be considered in developing the overall strategy.

(ii) *Risk assessment*: the application allows to identify the information system as one of the five components of internal control. It is required to obtain an understanding of the information system, including the procedures within both IT and manual systems. In other words, if s/he relies on internal control in assessing risk at an assertion level, s/he needs to understand and test the controls, whether these are manual or automated.

(iii) *Testing:* this stage is very important irrespective of the accounting system (any other internal reporting system), therefore it is useful to design the compliance and substantive tests that reflect the strengths and weaknesses of the system. When testing a computer information system, the it is likely to use a mix of manual and computer-assisted review and monitoring tests. 'Round the machine' vs. 'through the machine ' approaches to testing.

(iv) *Conclusion:* the key objectives of a review and control process is to obtain an understanding of the system in order to assess control risk and plan any review and mitigation process to minimize and/or detect risks. The assessment of the key controls will determine the level of internal testing. If these are programmed controls, you will need to 'review through the computer' and use CAATs to ensure controls are operating effectively. When auditing small computer-based systems, 'reviewing round the computer' may suffice if proper and reliable audit evidence can be obtained by testing input and output.

Conclusion

During the past recent years, the computer assisted risk assessments techniques was developed especially for large companies in various fields of activities such as banking, financial companies or retail stores. These are increasingly growing in importance and are helping in achieving a true and fair view over the financial results and mitigate the risks that might occur.

References:

1. http://www.barclaysimpson.com/document_uploaded/Introduction%20to%20Computer%20Audit.pdf
2. http://www.deloitte.com/view/en_GR/gr/services/enterprise-risk-services/it-control-assurance/information-systems-and-controls-audit/index.htm
3. www.accaglobal.com